IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

MITCHELL LAUTMAN on behalf of himself and all others similarly situated, Plaintiff, v. AMERICAN BANK SYSTEMS, INC., Defendant.	)	Case No. 2:20-cv-1959

CLASS ACTION COMPLAINT

Plaintiff Mitchell Lautman ("Plaintiff"), brings this Class Action Complaint, on behalf of himself and all others similarly situated (the "Class"), against Defendant**,** American Bank Systems, Inc. ("ABS" or "Defendant"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to her, which are based on personal knowledge:

NATURE OF THE CASE

1. Plaintiff brings this class action against ABS for ABS's failure to properly secure and safeguard protected personally identifiable information, including without limitations, names, dates of birth, phone numbers, addresses, bank account and loan information, and social security numbers (collectively, "PII"), for failing to comply with industry standards to protect information systems that contain PII, and for failing to provide timely, accurate, and adequate notice to Plaintiff and other Class Members that their PII had been compromised. Plaintiff seeks, among other things, damages, orders requiring ABS to fully and accurately disclose the nature of the information that has been compromised and to adopt reasonably sufficient security practices

and safeguards to prevent incidents like the disclosure in the future, and for ABS to provide identity theft protective services to Plaintiff and Class Members for their lifetimes, as Plaintiff and Class Members will be at an increased risk of identity theft due to the conduct of ABS described herein.

2. ABS is a third-party vendor that provides compliance and document management solutions services to over 350 financial institutions in 35 states, which financial institutions serve many customers across the United States.

3. In the course of doing business with ABS, financial institutions implement ABS's software on their systems. In turn, ABS maintains credentialing information for financial institutions, and ABS comes into possession of files containing the PII of financial institutions' customers and members.

4. One of ABS's financial institution customers, Pennsylvania-based NexTier Bank ("NexTier"), notified its banking customers, including Plaintiff, that their PII that had been stored on ABS's systems was exfiltrated by unauthorized third parties (the "Data Breach"). An exemplar of the Data Breach notification is attached hereto as "Exhibit A."

5. Since the Data Breach, other financial institutions have issued similar notices, indicating that their customers also had PII compromised in the wide-reaching Data Breach.

6. As a result of ABS's failure to implement and follow basic security procedures, Plaintiff's and Class Members' PII is now in the hands of criminals. Plaintiff and Class Members face a substantial increased risk of identity theft, both currently and for the indefinite future. Consequently, Plaintiff and Class Members have had to spend, and will continue to spend, significant time and money in the future to protect themselves due to ABS's failures.

7. Plaintiff, on behalf of himself and all others similarly situated, alleges claims for negligence, negligence *per se*, unjust enrichment, and declaratory judgment. Plaintiff seeks damages and injunctive relief, including the adoption reasonably sufficient practices to safeguard PII that remains in ABS's custody in order to prevent incidents like the Data Breach from reoccurring in the future.

PARTIES

8. Plaintiff Mitchell Lautman is a citizen and resident of the Commonwealth of Pennsylvania. At all times relevant to this Complaint, Plaintiff was a customer or NexTier, whose PII was disclosed without authorization to unknown third parties as a result of the ABS Data Breach.

9. Plaintiff received a letter from NexTier stating that ABS, one of NexTier's vendors, experienced a data security incident and unauthorized third parties were able to view and acquire data from ABS containing his PII.

10. Since the announcement of the Data Breach, Plaintiff has been required to spend his valuable time monitoring his various accounts in an effort to detect and prevent any misuses of his PII – time which he would not have had to expend but for the Data Breach.

11. As a result of the Data Breach, Plaintiff will continue to be at heightened risk for fraud and identity theft, and their attendant damages for years to come.

12. Defendant American Bank Systems, Inc. is an Oklahoma corporation that provides document management and compliance software solutions to the financial services industry. Defendant's registered address for service of process is 14000 Parkway Commons Drive, Oklahoma City, OK, 73134, and its principal place of business is at the same location.

JURISDICTION AND VENUE

13. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because Plaintiff and at least one member of the Class, as defined below, is a citizen of a different state than Defendant, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interests and costs.

14. This Court has personal jurisdiction over Defendant because at all relevant times it has engaged in substantial business activities, including the sale of financial systems management services, in Pennsylvania. Defendant has, at all relevant times, transacted, solicited, and conducted business in Pennsylvania through its employees, agents, and/or sales representatives, and derived substantial revenue from such business in Pennsylvania. Further, the claims alleged herein arise specifically from Defendant's provision of financial systems management services to NexTier Bank, a Pennsylvania-based financial institution.

15. Pursuant to 28 U.S.C. § 1391(b)(2), venue is proper in this District because a substantial part of the events or omissions giving rise to the claims occurred in this District.

FACTUAL BACKGROUND

American Bank Systems

16. ABS markets itself as having "created advanced management systems for the financial industry that help assess, monitor and lower compliance risk"[1] and being "[t]he bank systems software suite most trusted by banking professionals."[2]

[1] https://www.americanbanksystems.com/about/
[2] https://www.americanbanksystems.com/banking-systems/

17. ABS's software product offerings include BankManager, CreditUnionPro, CompliancePro, and CoPilot Loans and Deposits. These programs perform a variety of functions, including streamlining lending processes through document tracking and storage management, linking customer accounts and data across multiple systems, report generation, compliance monitoring, and other similar services.

18. Defendant currently "is serving more than 350 banks, credit unions and other financial institutions in 35 states – and counting."[3]

19. As part of its relationship with financial institutions, ABS routinely acquires and stores the financial institutions' customers' PII on its systems. Financial institutions save time and money by using ABS's services by not having to pay the cost of in-house compliance personnel or maintaining the systems and infrastructure required of a dedicated server.

20. Financial institution customers demand security to safeguard their PII. As a vendor storing sensitive financial related data, ABS is required to ensure that such private, sensitive information is not disclosed or disseminated to unauthorized third parties.

Background on Ransomware Attacks and Avaddon

21. Ransomware is a well-known and increasingly common form of cyberattack in which the attacker introduces malware to the target's systems. The malware then uses encryption methods to block the victim from using or accessing the targeted system or data.

22. The malware is typically introduced to the victim's systems through a relatively unsophisticated route: malicious "Trojan" emails sent to specific users who have access to the target's systems. The emails include attachments disguised as ordinary excel files, jpegs, or zip drives, or links that appear to be for package tracking or other innocent purposes. If the user

[3] https://www.americanbanksystems.com/about/

opens the malicious attachment or clicks the link and allows it to download an application, a program will open that either unpacks the ransomware directly or allows the attackers gain a foothold in the system to launch further attacks.

23. Once the ransomware is in place, the malware typically includes instructions for contacting the attacker, who then offers to remove the malware or provide a decryption key in exchange for payment, often in the form of Bitcoin or another cryptocurrency. In some instances, referred to by some as "double extortion," the attacker also exfiltrates sensitive data and threatens to release it to the public, or sell it on the "dark web," if the ransom demands are not met.

24. The number of ransomware attacks increased dramatically during the 2010s, and some well-known variants, such as WannaCry, Locky, and Petya, have been used in thousands of separate attack incidents. Targets have included all sizes of businesses in virtually every sector, non-profits including hospitals and universities, and government agencies.

25. Beginning in or around July 2020, a cybercrime news publication described a new variant of ransomware called Avaddon.[4] The report identified that the typical delivery route was, like most other malware attacks, a Trojan email with a malicious attachment, with subject lines suggesting that the attachment contained a photograph of the recipient.[5]

26. The news report also described how the malicious file unloads the ransomware to the user's system, which system folders are targeted for encryption, and alterations the

[4] Trend Micro, *Ransomware Report: Avaddon and New Techniques Emerge, Industrial Sector Targeted*, July 8, 2020 (updated July 23, 2020), available at: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-report-avaddon-and-new-techniques-emerge-industrial-sector-targeted

[5] *Id.*

ransomware makes to running Windows processes and services.[6] The article also included examples of a desktop image the ransomware places on the user's computer which points the user to the "ransom note," which in turn describes how the victim can contact the attackers in order to "buy" a decryption program.[7]

27. Another data security blog reported in August 2020 that the operators of Avaddon set up their own website on which to publish leaked data whenever a victim failed to pay ransom.[8]

The ABS Data Breach

28. In early November 2020, the group purporting to be behind the Avaddon malware attacks published a "leak warning" claiming that they had hacked ABS and taken possession of over 50 gigabytes of data. The group demanded a ransom in exchange for release of the data, coupled with a threat of public disclosure.[9]

29. The group claimed that ABS "do not want to pay and think[] that we are bluffing." The group contemporaneously leaked four gigabytes of the stolen data.[10]

30. Analysis by one news outlet indicated that the sample leak included a variety of highly sensitive information, such as loan documents, login credentials for financial institutions' internal file sharing networks, and financial records. In turn, some of the leaked financial documents included banking customers' PII, including names, social security numbers, loan amounts, interest rates, and pertinent loan dates such as origination dates, maturity dates, and pay

---

[6] *Id.*
[7] *Id.*
[8] https://cofense.com/avaddon-ransomware-joins-data-exfiltration-trend/
[9] https://securityreport.com/american-bank-systems-hit-by-ransomware-attack-full-53-gb-data-dump-leaked/?web_view=true
[10] *Id.*

off dates. Astonishingly, much of this sensitive data appears to have been stored by ABS in unencrypted, plaintext files – meaning that anyone who gained access to the files could fully read the information (and sensitive PII) therein.[11]

31. The article indicated that, based on timestamps on screenshots of the leaked files, the breach initially began "sometime in or before early October."[12]

32. ABS apparently did not pay the ransom, and by November 14, 2020 the full 52.57 gigabytes of stolen data, including Plaintiff's and the Class Members' PII, in the Avaddon group's possession was leaked.[13]

33. According to NexTier Bank, it was not notified by ABS of the Data Breach until November 18, 2020, which was at least several weeks after the incident began, and more than two weeks after the Data Breach was first publicly reported.

Financial Information is Particularly Vulnerable to Data Breaches

34. ABS, a company that promotes its trustworthiness, has a responsibility to securely maintain the customer PII that it receives and keep it safe from harm. ABS was on notice that PII, specifically when it includes financial information, is a prime target for data breaches.

35. "Due to the nature of these businesses and the sensitivity of their data, financial firms are hit with approximately 300 times more cyber attacks than businesses in other industries."[14]

---

[11] *Id.*
[12] *Id.*
[13] *Id.*
[14] https://www.bitsight.com/blog/financial-data-breaches-2019-capital-one-first-american-desjardins-more

36. "In 2018 the sector reported 819 cyber incidents, a significant increased from the 69 incidents report in 2017."[15]

37. "Banks and financial services organizations were the targets of 25.7 percent of all malware attacks last year, more than any other industry."[16]

38. Particularly during Covid-19, while employees are working remotely, cybercriminals are working to exploit fear and uncertainty. From February to April 2020, cyber attacks in the financial sector increased by 238 percent.[17]

39. ABS knew, or should have known, the importance of safeguarding Plaintiff and Class Members' PII entrusted to it by financial institutions around the country and knew, or should have known, the foreseeable consequences if that data was disclosed. This includes the significant costs that would be imposed on patients as a result of a breach. ABS failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

ABS Obtains, Collects, and Stores Plaintiff's and Class Members' PII

40. In the ordinary course of doing business with ABS's customers—financial institutions—Plaintiff and Class Members are regularly required to provide their sensitive, personal and private protected information in order to open accounts, obtain loans, and perform other financial activities.

41. Due to ABS's role as a third-party vendor for financial institutions, Plaintiff and Class Members have no direct contractual relationship with ABS, and were generally unaware that ABS had access to Plaintiff and Class Members' PII.

---

[15] *Id.*
[16] https://www.forbes.com/sites/zakdoffman/2019/04/29/new-cyber-report-25-of-all-malware-hits-financial-services-card-fraud-up-200/?sh=a15e9e17a47a
[17] https://www.helpnetsecurity.com/2020/06/17/cybercriminals-sophisticated/

42. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, ABS assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

43. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and they reasonably expect that vendors who work with their financial institutions will use the utmost care to keep this information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

44. ABS acknowledges the seriousness of protecting personal information. As stated in Defendant's Privacy Policy:

> We take our users' privacy very seriously. We feel that certain personal information should always be kept private. We have technology measures to protect any personal information you submit from misuse and loss, such as firewalls and password-protected areas using established industry standards. These measures are also designed to protect personal information from unauthorized access, modification, and disclosure. However, no data protection measures are entirely foolproof when data is transmitted and stored over the Internet.

45. Despite Defendant's commitment to protecting personal information, ABS failed to prioritize data and cyber security by adopting reasonable data and cyber security measures to prevent and detect the unauthorized access to Plaintiff's and Class Members' PII.

46. Had ABS remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, ABS could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential PII.

The Value of Private Information and Effects of Unauthorized Disclosure

47. ABS was well aware that the protected financial information and PII it touches is highly sensitive and of significant value to those who would use it for wrongful purposes.

48. PII is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identity theft, and medical and financial fraud.[18] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII and other protected financial information on multiple underground Internet websites, commonly referred to as the "dark web."

49. While PII is valued at approximately $1 per line of information, "Bank account credentials can sell for anywhere between $200 and $500 apiece. . . ."[19]

50. Protected financial information is particularly valuable because criminals can use not only a person's personal information for identity theft, but can also gain access to bank accounts and cash contained therein.

51. "Financial identity theft is a significant crime, and potentially one of the more damaging types of identity theft. Consider the possibilities – an identity thief gaining access to your bank accounts or retirements accounts and stealing your hard-earned money."[20]

52. The ramifications of ABS's failure to keep Plaintiff and Class Members' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

[18] https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft
[19] https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft
[20] https://www.lifelock.com/learn-identity-theft-resources-what-is-financial-identity-theft.html

53. Further, criminals often trade stolen PII on the "cyber black market" for years following a breach. Cybercriminals can also post stolen PII on the internet, thereby making such information publicly available.

54. ABS knew, or should have known, the importance of safeguarding the PII entrusted to it and of the foreseeable consequences if its data security systems were breached. ABS failed, however, to take adequate cyber security measures to prevent the Data Breach from occurring.

FTC Guidelines

55. ABS is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

56. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[21]

57. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understands their network's vulnerabilities, and implement policies to correct any security problems.[22]

[21] https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf
[22] https://www.ftc.gov/system/files/documents/plain-language/pdf-0136proteting-personal-information.pdf.

58. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[23]

59. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

60. ABS failed to properly implement basic data security practices. ABS's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

61. ABS was at all times fully aware of its obligations to protect the PII of consumers because of its position as a compliance solutions provider for financial institutions, which gave it direct access to consumer PII. ABS was also aware of the significant repercussions that would result from its failure to do so.

Plaintiff and Class Members Suffered Damages

62. The ramifications of ABS's failure to keep PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for

[23] *Id.*

years. Consumer victims of data breaches are more likely to become victims of identity fraud, occurring 65 percent of the time.[24]

63. In 2019 alone, consumers lost more than $1.9 billion to identity theft and fraud.[25]

64. Besides the monetary damage sustained, consumers may also spend anywhere from approximately 7 hours to upwards of 1,200 hours trying to resolve identity theft issues.[26]

65. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

66. Despite all of the publicly available knowledge of the continued compromises of PII, ABS's approach to maintaining the privacy of protected financial information and other PII was reckless, or in the very least, negligent.

67. As a result of ABS's failure to prevent the Data Breach, Plaintiff and Class Members have suffered and will continue to suffer injuries, including loss of time and productivity through efforts to ameliorate, mitigate, and deal with the future consequences of the Data Breach; theft of their valuable PII; the imminent and certain impeding injury flowing from fraud and identity theft posed by their PII being placed in the hands of criminals; damages to and diminution in value of their PII that was entrusted to Defendant with the understanding the Defendant would safeguard the PII against disclosure; and continued risk to Plaintiff's and the

[24] https://www.identityforce.com/blog/identity-theft-odds-identity-theft-statistics#:~:text=In%202019%2C%2014.4%20million%20consumers,about%201%20in%2015%20people&text=Identity%20theft%20is%20the%20most,data%20breaches%20increased%20by%2017%25

[25] *Id.*

[26] https://www.lifelock.com/learn-identity-theft-resources-how-long-does-it-take-to-recover-from-identity-theft.html#:~:text=And%20ID%20theft%20recovery%20is,more%20resolving%20identity%20theft%20problems.

Class Members' PII, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate an adequate measures to protect the PII that was entrusted to it.

CLASS ALLEGATIONS

68. Plaintiff brings this case individually and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the class defined as:

> All individuals in the United States whose PII was compromised in the American Bank Systems Data Breach which occurred between October and November, 2020.

69. Excluded from the Class is Defendant, their subsidiaries and affiliates, their officers, directors and members of their immediate families and any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

70. Plaintiff reserves the right to modify or amend the definition of the proposed Class if necessary before this Court determines whether certification is appropriate.

71. The requirements of Rule 23(a)(1) are satisfied. The class described above is so numerous that joinder of all individual members in one action would be impracticable. The disposition of the individual claims of the respective class members through this class action will benefit both the parties and this Court. The exact size of the class and the identities of the individual members thereof are ascertainable through Defendant's records, including but not limited to, the files implicated in the Data Breach.

72. The requirements of Rule 23(a)(2) are satisfied. There is a well-defined community of interest and there are common questions of fact and law affecting members of the

Class. The questions of fact and law common to the Class predominate over questions which may affect individual members and include the following:

a. Whether and to what extend Defendant had a duty to protect the PII of Plaintiff and Class Members;

b. Whether Defendant was negligent in collecting and storing Plaintiff's and Class Members' PII;

c. Whether Defendant had duties not to disclose the PII of Class Members to unauthorized third parties;

d. Whether Defendant took reasonable steps and measures to safeguard Plaintiff's and Class Members' PII;

e. Whether Defendant failed to adequately safeguard the PII of Class Members;

f. Whether Defendant breached its duties to exercise reasonable care in handling Plaintiff's and Class Members' PII by storing that information unencrypted on computers and hard drives in the manner alleged herein, including failing to comply with industry standards;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant had respective duties not to use the PII of Class Members for non-business purposes;

i. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

j. Whether Plaintiff and Class Members are entitled to damages as a result of Defendant's wrongful conduct;

k. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

l. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

73. The requirements of Rule 23(a)(3) are satisfied. Plaintiff's claims are typical of the claims of the members of the Class. The claims of the Plaintiff and members of the Class are based on the same legal theories and arise from the same failure by Defendant to safeguard PII.

74. Plaintiff and members of the Class were each customers of financial institutions that were clients of ABS, each having their PII obtained by an unauthorized third party.

75. The requirements of Rule 23(a)(4) are satisfied. Plaintiff is an adequate representative of the class because his interests do not conflict with the interests of the members of the Class. Plaintiff will fairly, adequately, and vigorously represent and protect the interests of the members of the Class and has no interests antagonistic to the members of the Class. In addition, Plaintiff has retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiff and the Class members are substantially identical as explained above. While the aggregate damages that may be awarded to the members of the Class are likely to be substantial, the damages suffered by the individual members of the Class are relatively small. As a result, the expense and burden of individual litigation make it economically infeasible and procedurally impracticable for each member of the Class to individually seek redress for the wrongs done to them. Certifying the case as a Class will centralize these substantially identical claims in a single proceeding, which is the most

manageable litigation method available to Plaintiff and the Class and will conserve the resources of the parties and the court system, while protecting the rights of each member of the Class. Defendant's uniform conduct is generally applicable to the Class as a whole, making relief appropriate with respect to each Class member.

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

76. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

77. ABS owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their PII in its possession from being compromised, lost, stolen, accessed and misused by unauthorized persons. More specifically, this duty including, among other things: (a) designing, maintaining, and testing ABS's security systems to ensure that Plaintiff's and Class Members' PII in ABS's possession was adequately secured and protected; (b) implementing processes that would detect a breach of its security system in a timely manner; (c) timely acting upon warning and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data security measures consistent with industry standards.

78. ABS's duty to use reasonable care arose from several sources, including but not limited to those described below.

79. ABS had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendant. By collecting and storing valuable PII

that is routinely targeted by criminals for unauthorized access, ABS was obligated to act with reasonable care to protect against these foreseeable threats.

80. ABS's duty also arose from ABS's position as a financial institution vendor. ABS undertakes its collection of highly sensitive information generally without the knowledge or consent of consumers and consumers cannot "opt out" of ABS's data collection activities. ABS holds itself out as a trusted steward of consumer data, and thereby assumes a duty to reasonably protect that data. The consumer public have no choice but to repose a trust and confidence in ABS to perform that stewardship carefully. Otherwise consumers would be powerless to fully protect their interests with regard to their PII, which is controlled by ABS. Because of its crucial role within the financial system, ABS was in a unique and superior position to protect against the harm suffered by Plaintiff and Class Members as a result of the ABS Data Breach.

81. ABS admits that it has the responsibility to protect consumer data, that it is entrusted with this data, and that it did not live up to its responsibility to protect the PII at issue here.

82. ABS breached the duties owed to Plaintiff and Class Members and thus was negligent. ABS breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII of Plaintiff and Class Members; (b) detect the breach while it was ongoing; (c) maintain security systems consistent with industry standards; and (d) disclose that Plaintiff's and Class Members' PII in ABS's possession had been or was reasonably believed to have been, stolen or compromised.

83. But for ABS's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII would not have been compromised.

84. As a direct and proximate result of ABS's negligence, Plaintiff and Class Members have suffered injuries, including:

a. Theft of their PII;

b. Costs associated with requested credit freezes;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

d. Costs associated with purchasing credit monitoring and identity theft protection services;

e. Unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects of their credit;

f. Lowered credit scores resulting from credit inquiries following fraudulent activities;

g. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the ABS Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

h. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

i. Damages to and diminution in value of their PII entrusted, directly or indirectly, to ABS with the mutual understanding that ABS would safeguard Plaintiff's and Class Members data against theft and not allow access and misuse of their data by others; and

j. Continued risk of exposure to hackers and thieves of their PII, which remains in ABS's possession and is subject to further breaches so long as ABS fails to undertake appropriate and adequate measures to protected Plaintiff.

85. As a direct and proximate result of ABS's negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE PER SE
(On Behalf of Plaintiff and the Class)

86. Plaintiff restates and realleges all proceeding factual allegations above as if fully set forth herein.

87. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as ABS or failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of ABS's duty.

88. ABS violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect PII and not complying with the industry standards. ABS's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach within the financial industry.

89. ABS's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

90. Plaintiff and Class Members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect.

91. Moreover, the harm that has occurred is the type of harm that the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

92. As a direct and proximate result of ABS's negligence, Plaintiff and Class Members have been injured as described herein and in Paragraph 84 above, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

93. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

94. Plaintiff and Class Members have an interest, both equitable and legal, in the PII about them that was conferred upon, collected by, and maintained by ABS and that was ultimately stolen in the ABS Data Breach.

95. ABS was benefitted by the conferral upon it of the PII pertaining to Plaintiff and Class Members and by its ability to retain and use that information. ABS understood that it was in fact so benefitted.

96. ABS also understood and appreciated that the PII pertaining to Plaintiff and Class Members was private and confidential and its value depended upon ABS maintaining the privacy and confidentiality of that PII.

97. But for ABS's willingness and commitment to maintain its privacy and confidentiality, that PII would not have been transferred to and entrusted with ABS. Further, if ABS had disclosed that its data security measures were inadequate, ABS would not have been permitted to continue in operation by regulators and participants in the marketplace.

98. As a result of ABS's wrongful conduct as alleged in this Complaint (including among other things its utter failure to employ adequate data security measures, its continued maintenance and use of the PII belonging to Plaintiff and Class Members without having adequate data security measures, and its other conduct facilitating the theft of that PII), ABS has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and Class Members.

99. ABS's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiff's and Class Members' sensitive PII, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identify thieves.

100. Under the common law doctrine of unjust enrichment, it is inequitable for ABS to be permitted to retain the benefits it received, and is still receiving, without justification, from the use of Plaintiff and Class Members' PII in an unfair and unconscionable manner. ABS's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

101. The benefit conferred upon, received, and enjoyed by ABS was not conferred officiously or gratuitously, and it would be inequitable and unjust for ABS to retain the benefit.

102. ABS is therefore liable to Plaintiff and Class Members for restitution in the amount of the benefit conferred on ABS as a result of its wrongful conduct, including specifically the value to ABS of the PII that was stolen in the ABS Data Breach and the profits ABS received from the use of that information.

FOURTH CAUSE OF ACTION
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Class)

103. Plaintiff restates and realleges all proceeding allegations above as if fully set forth herein.

104. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

105. An actual controversy has arisen in the wake of the ABS Data Breach regarding Plaintiff's and Class Members' PII and whether ABS is currently maintaining data security measures adequate to protect Plaintiff's and Class Members from further data breaches that compromise their PII. Plaintiff alleges that ABS's data security measures remain inadequate. ABS denies these allegations. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of his PII and remains at imminent risk that further compromises of his PII will occur in the future.

106. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. ABS owes a legal duty to secure consumers' PII and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes; and

b. ABS continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII.

107. This Court also should issue corresponding prospective injunctive relief requiring ABS to employ adequate security protocols consistent with law and industry standards to protect consumers' PII.

108. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at ABS. The risk of another such breach is real, immediate, and substantial. If another breach at ABS occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

109. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to ABS if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to ABS of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and ABS has a pre-existing legal obligation to employ such measures.

110. Issuance of the requested injunction will not disserve the public interest. To the contract, such an injunction would benefit the public by preventing another data breach at ABS, thus eliminating the additional injuries that would result to Plaintiff and consumers whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE Plaintiff on behalf of himself and all other similarly situated, prays for relief as follows:

a. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

b. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

c. For damages in an amount to be determined by the trier of fact;

d. For an order of restitution and all other forms of equitable monetary relief;

e. Declaratory and injunctive relief as described herein;

f. Awarding Plaintiff's reasonable attorneys' fees, costs, and expenses;

g. Awarding pre- and post-judgment interest on any amounts awarded; and,

h. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMAND

A jury trial is demanded on all claims so triable.

Dated: December 16, 2020

Respectfully submitted,

/s/ Gary F. Lynch

Gary F. Lynch (PA ID 56887)
CARLSON LYNCH, LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
T: (412) 322-9243
F: (412) 231-0246
glynch@carlsonlynch.com

Counsel for Plaintiff